استخدام العلامة المائية في اخفاء البيانات

اعداد
سارة علاء شاكر

اشراف
الاستاذ عصام سرحان

نيسان ٢٠١٠ ١٤٣٠

الفصل الاول

المقدمة

علم الإخفاء لا يعد من العلوم المستحدثة، فلقد كان أول ظهور لهذا العلم في العصر الإغريقي، حيث قام أحد رجالات العصر بالتواصل مع احد أقربائه في اليونان، عن طريق حلق شعر رؤوس عبيده ثم وشم الرسائل على رؤوسهم بعد ذلك يقوم بانتظار نمو شعر رأسهم ثم إرسالهم إلى الشخص الذي يهدف إلى التواصل معه. ثم جاء بعده العديد من الأشخاص الذين استخدموا الناس والحيوانات والخشب المغطى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية. واستمر تطور هذا العلم، حتى توصل العالم إلى اختراع الحبر الخفي إبان الحرب العالمية الثانية، والذي ساهم كثيراً في التواصل بين أطراف الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الإسرار. وقد تطور علم الإخفاء في الوقت الحالي كثيراً، فأصبح يستخدم المعلومات الرقمية والكمبيوترات كوسيلة لنقل البيانات. وتذكر كارين كورهورن (Karen Korhorn) إن المنظمة العالمية لحقوق الإنسان قد جمعت حوالي ٥٠٠٠ شهادة، من شهود عيان، عن طريق استخدام هذه التقنية مع التشفير، فحصلت على المعلومات وحافظت على حياة الشهود.

ان إخفاء المعلومات هو فنُ و علمُ و كتابة الرسائل الخفية بطريقةٍ لا تسمح لأحدٍ بالوصول إلى فهم الموجود في الرسالة، ما عدى المرسل و المتلقي المقصود، و هو شكلٌ من أشكال الأمن من خلال الغموض.ويسمى هذا الفن (الستيجانوغرافيا) تأتي كلمة *ستيجانوجرافي* من أصلٍ يوناني و تعني *"الكتابة المخفية"*. أول استخدامٍ تم تسجيله لهذا المصطلح هو في عام ١٤٩٩، و ذلك من قبل يوهانس تريثيمياس في تقريره *الستيجانوجرافيا* ، و هي أطروحة عن التشفير و إخفاء المعلومات تم تنكيرها لتبدو ككتاب عن السحر. عامةً ما تبدو الرسائل كشيءٍ آخر: كصور أو مقالات أو قوائم تسوق، أو بعض الأنواع الأخرى من *النصوص الخافية* ، و تكون الرسالة المخبأة بشكل تقليدي مكتوبة بحبرٍ غير مرئي بين الخطوط الواضحة في رسالةٍ خاصة.

ميزة الستيجانوجرافي على الكريبتوجرافي (التشفير) وحده، هو أن الرسائل لا تلفت النظر إلى نفسها. فالرسائل المشفرة المرئية بوضوح -مهما كانت صعوبة فك شيفرتها- يمكن أن تثير الشكوك، و ربما تكون في حد ذاتها إدانة في البلدان التي يكون التشفير فيها أمرا غير قانوني. لذا، في حين يحمي التشفير محتويات الرسالة، يقوم "إخفاء الكتابة" بحماية كل الأطراف ورسائل الاتصال

يتضمن الستيجانوجرافي إخفاء المعلومات داخل ملفات الكمبيوتر. في الكتابة المخفية الرقمية، يمكن أن تشمل الاتصالات الالكترونية الترميز الستيجانوجرافي داخل طبقة نقل، مثل ملف وثيقةٍ أو ملف صورةٍ أو برنامجا أو بروتوكولا. و ملفات الوسائط هي مثالية للانتقال الستيجانوجرافي بسبب حجمها الكبير. كمثال بسيط، يمكن لمرسلٍ أن يبدأ بملف صورةٍ حميدةٍ ثم يقومُ بضبط اللون في كل بكسلٍ بعد مائة بكسل ليتوافق مع حرفٍ في الأبجدية، و هذا تغير ماكرٌ بحيث ألا يلحظه شخصٌ لا يبحث عنه خصيصا. لم يبحث على وجه التحديد لأنه من غير المرجح أن تلاحظ ذلك.

أول استخدام مسجلٍ للستيجانوجرافي يمكن إرجاعه الى ٤٤٠ قبل الميلاد عندما يذكر هيرودوت مثالين على "إخفاء المعلومات" في *تواريخ هيرودوت*. أرسل ديماراتاس تحذيرا حول هجومٍ وشيك الى اليونان عن طريق كتابته مباشرةً على الدعامة الخشبية لقرصٍ من الشمع قبل وضع سطحية شمع العسل فوقها. كانت أقراص الشمع شائعة الاستعمال في الكتابة لإمكانية إعادة استخدام سطوحها، و كان يتم أحيانا استخدامها للكتابة الاختزال. و مثالٌ قديمٌ آخرُ هو هيستييس، الذي حلق رأس عبده الذي يثق فيه أكثر من غيره، و وشم رسالة على رأسه. و بعد نمو شعر رأسه أصبحت الرسالة مخبأة. و كان الغرض من ذلك التحريض على التمرد ضد الفرس.

كان إخفاء المعلومات يستخدم على نطاق واسع، بما في ذلك العصور التاريخية الماضية و حتى يومنا هذا. التباديل الممكنة لا حصر لها و تشمل أمثلتها المعروفةُ الآتي:

ساره علاء شاكر



على سبيل المثال. ضمن هذه الصورة ، موقف خطابات رسالة خفية يتم تمثيل الأعداد المتزايدة (من ١ إلى ٢٠) ، وقيمة الرسالة التي قدمها موقفها تقاطع في الشبكة. على سبيل المثال ، أول حرف من الرسالة الخفية هو عند تقاطع ١ و ٤. لذلك ، وبعد محاولات عدة ، أول حرف من الرسالة ويبدو أن هذه الرسالة th١٤ من الأبجدية ، وآخر واحد (رقم ٢٠) هو حرف من الحروف الأبجدية th٥.

- الرسائل المخفية داخل أقراص الشمع: في اليونان القديمة، كان الناس يكتبون الرسائل على الخشب، ثم يغطونها بشمعٍ عليه رسالةٌ أخرى بريئة.
- الرسائل الخفية على أجساد الرُسُل: كانت تستخدم أيضا في اليونان القديمة. يروي هيرودوت قصة وشمٍ مطبوع على رأس عبدٍ من العبيد بعد حلق رأسه، و أصبحت الرسالة مخفيةً بعد نمو الشعر مرةً أخرى. يزعم أن الرسالة كانت تحذيرا إلى اليونان حول خطط غزوٍ فارسية. كان لهذا الأسلوب عيوبٌ واضحةٌ مثل الانتقال المتأخر في انتظار عودة الشعر بعد نموه، و إمكانية استخدام الرأس لمرةٍ واحدةٍ فقط. في الحرب العالمية الثانية، أرسلت المقاومة الفرنسية بعض الرسائل المكتوبة على ظهر السعاة بالحبر السري.
- رسائل خفية على ورقةٍ مكتوبةٍ بالأحبار السرية، في إطار رسائل أخرى أو على أجزاءٍ فارغةٍ من رسائل أخرى.
- الرسائل المكتوبة برموز مورس على الغزل ثم خياطتها على قطعةٍ من الملابس التي يرتديها ساعي.
- الرسائل المكتوبة على الجزء الخلفي من الطوابع البريدية.
- أثناء و بعد الحرب العالمية الثانية، استخدم عملاء الجاسوسيةالنقاط الدقيقة المنتجة فوتوغرافيا لإرسال المعلومات جيئةً و ذهابا. عادةً ما كانت النقاط الدقيقة (مايكرودوتس) أقل من حجم الحروف التي تنتجها الآلة الكاتبة. كان ينبغي وضع "المايكرودوتس" في الحرب العالمية الثانية في ورقةٍ و تغطيتها بلاصق (مثل الكولوديون). و كان هذا عاكسا للضوء، مما يمكن قراءة الرسالة عن طريق وضعها أمام الضوء. كان من التقنيات البديلة إدراج "المايكرودوتس" في شقوقٍ تم تقطيعها في حافة البطاقات البريدية.
- خلال الحرب العالمية الثانية، بعث جاسوسٌ لصالح اليابان في مدينة نيويورك، فيلفالي ديكينسون، معلوماتٍ إلى عناوين مواقع محايدة في أمريكا الجنوبية. كانت العناوين لبائعة دمى، و كانت رسائلها تناقش عدد الدمى التي يجب عليها شحنها. كان النص المخفي أسماء الدمى، في حين أن النص 'المشفر' المخفي كان معلوماتٍ حول تحركات السفن، وما إلى ذلك. أصبحت قضيتها مشهورةً نوعا ما، و أصبحت تعرف باسم امرأة الدمى.
- الدعاية المضداة في الحرب البارد. في عام ١٩٦٨، كان أفراد طاقم سفينة الاستخبارات بويبلو (آجر - ٢) المحتجزين كأسرى من جانب كوريا الشمالية يبلغون رسائل بلغة الإشارة حين فرص التقاط الصور، التي تخبر الولايات المتحدة أنهم لم يكونوا منشقين بل كانوا محتجزين من قبل الكوريين الشماليين . في صورٍ أخرى تم تقديمها إلى الولايات المتحدة، أشار أفراد الطاقم "بأصابعهم" نحو الكوريين أثناء انشغالهم، في محاولةٍ لتشويه الصور التي أظهرتهم مبتسمين و مرتاحين.

دخلت الستيجانوجرافيا الحديثة إلى العالم في عام ١٩٨٥ مع ظهور الكمبيوتر الشخصي و استخدامه في حل مشاكل إخفاء المعلومات الكلاسيكية. كان التطور بعد ذلك بطيئا، و لكنه انطلق كثيرا منذ ذلك الحين، بعدد برامج "الستي جو" المتاحة: تم تحديد أكثر من ٧٢٥ تطبيقا ستيجانوجرافيا رقميا من قبل مركز تحليل و أبحاث الستيجانوجرافيا. تشمل التقنيات الرقمية لإخفاء المعلومات ما يلي:

- إخفاء الرسائل داخل البتات الأدنى في الصور الصاخبة أو ملفات الصوت.
- إخفاء البيانات ضمن البيانات المشفرة أو ضمن البيانات العشوائية. يتم تشفير البيانات التي يراد إخفاؤها قبل استخدامها لاستبدال جزءٍ من كتلةٍ أكبر بكثيرٍ من البيانات المشفرة أو كتلةٍ من البيانات العشوائية (فالشفرات غير قابلة للفك مثل وسادة المرة الواحدة تستطيع توليد نصوص مشفرة تبدو عشوائية تماما إذا لم يكن لديك مفتاحها الخاص).
- الممازحة و التذرية.
- تحول الوظائف المُقلِدَة ملفا واحدا لتحطيه البيانات الإحصائية لملفٍ آخررى. يمكن أن يساعد هذا الأساليب الإحصائية التي تساعد هجمات "القوة الغاشمة" في تحديد الحل الصحيح في هجوم النصوص المشفرة فقط.
- الرسائل السرية في الملفات التنفيذية التي عُبث بها، مستغلة التكرار في مجموعة تعليمات i386.
- الصور المضمنة في محتوى فيديو (و التي يمكن تشغيلها اختياريا بسرعةٍ أبطأ أو أسرع).
- حقن تأخيراتٍ غير مدركة في حزمِ مرسلةٍ عبر الشبكة من لوحة المفاتيح. فالتأخير في الضغط على المفاتيح في بعض التطبيقات (التلنت أو البرمجيات المكتبية البعيدية) يمكن أن يعني تأخيرا في الحزم، و التأخير في الحزم يمكن استخدامه في ترميز البيانات.
- تخفي "الستيجانوجرافيا المدركة للمحتوى" المعلومات في الدلالات التي يسندها المستخدم البشري إلى حزم البيانات. توفر هذه النظم الأمن ضد الدخيل غير بشري.
- ستيجانوجرافيا البلوج. يتم تقطيع الرسائل و يتم إضافة القطع (المشفرة) كتعليقاتٍ لسجلات الشبكة المبتورة (أو اللوحات المعلقة على منصات الشبكات الاجتماعية). في هذه الحالة يعتبر اختيار البلوجات هو المفتاح المتماثل الذي يمكن للمرسل و المستلم استخدامه؛ و ناقل الرسالة الخفية هي المدونات بأكملها.

يمكن لمنتج الستيجانوجرافيا الرقمية أن يكون على شكل وثائق مطبوعة. يمكن أن تكون البداية *بتشفير* الرسالة، أي النص الواضح، بواسطة الوسائل التقليدية، ثم إنتاج *النص المشفر*. ثم يتم تعديل النص *الغطائي* الحميد بأي طريقةٍ لكي لا يحتوي على النص المشفر، مما يؤدي إلى تكوين *النص الستيجانوجرافي*. على سبيل المثال، يمكن التلاعب بحجم الرسالة و التباعد الذي فيها، أو بالمحرف، أو غيرها من خصائص النص الغطائي ليحملرسالة خفية. يمكن فقط للمتلقي الذي يعرف التقنية المستخدمة لاسترداد الرسالة يمكنه فك تشفيرها. طور فرانسيس بيكون شيفرة بيكون بهذا الاسلوب.

أهمية البحث

تعتبر الشبكة الدولية للمعلومات (الانترنيت) هي البيئة الجديدة للتعامل مع المعلومات في ثورة المعلومات ونتيجة لازديـاد أهميتها , برز التفكير الجاد في حمايتها وحماية خصوصية الأفراد العاملين عليها، لذلك لم تعد الأمنية موضـوعا متعلقـا بطرق التشفير ووضع السياسات الأمنية والبحث في الثغرات في بروتوكولات الاتصالات فحسب بل باتت تشمل أيضا محاولة الـسيطرة علـى محتـوى المعلومـات المتداولـة عبـر الانترنيـت وحـول العـالم .

تصب جميع التقنيات الحديثة في مجرى واحد ، هو سهولة الوصول إلى معلومة من قبل المستخدمين والذي أدى بلا شـك إلى انتهاك أمنيتها، أن المفهوم الجديد لنموذج تداول المعلومات يشير إلى انسيابية المعلومات باتجاه المستخدم من خـلال شبكة الانترنيت والوسائل المتاحة الأخرى وهذا يستدعي أعادة النظر بالنمـاذج المـستخدمة فـي أنظمـة المعلومـات.

ظهرالتشفير كطريقة الناجحة لحماية البيانات المخزونة والمتراسلة ، وكانت الفكرة بان الاتصالات قد تكون أمينة من خلال تشفير المرور. لكن هذا نادرا ما يكون صحيح في الواقع العملي،فبرزت الحاجة لإيجاد طرق لإخفاء الرسـائل بـدلا مـن تشفيرها ، لذلك تتضمن أمنية الاتصالات ليس فقط التشفير وإنما أيضا أمنية المرور التي يكون جوهرها موجود في أخفاء المعلومـــات.

تمثل تقنية أخفاء المعلومات الحبر السري للوثائق الرقمية ، أن أخفاء المعلومات يعني أخفاء معلومات في معلومات أخرى بريئـة المظهـر ولا تجلـب الانتبـاه.

الأهم في هذه التقنية الحديثة في توظيفها أنها غير واضحة للنظر إضافة إلى مرونتها في استخدام كافة الوسـائط لغـرض

الإخفاء حيث يمكن أخفاء الرسالة السرية بكافة أشكالها (صورة، صوت، نص) داخل أوعية معلومـــات تمتلــك خــصائص مختلفة(صوت، صورة، نص، وسائط متعددة)، وجعلها غير مدركة من قبل المتطفلين والمهاجمين وهكذا تكون المعلومـــات مجهولة لمستخدمين الشبكة بينما يبقى محتواها حكرا على الجهات ذات العلاقة والتي تعرف كيفية استخراج محتواها.

لإخفاء المعلومات أهمية كبيرة وذلك لأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عاملاً مساعداً على إضفاء حماية وأمناً على المعلومات. يستخدم هذا الفن في عدد من المجالات إلا أن المجال الذي يبرز فيه هذا الفن هو التجارة الإلكترونية التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد آخر. من تطبيقات هذا العلم، العلامات المائية (Watermarks) والتي تستخدم في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة. وبالرغم من أن المشتري أو مستخدم هذه البرامج قد يعلم بوجود مثل هذه العلامات، إلا أن اكتشاف أماكنها داخل البرنامج من الصعوبة بمكان. وعلى افتراض أن المستخدم قد تعرف على مكان وجود هذه العلامة، فسيظهر أمامه تحدٍ آخر، وهو معرفة البرنامج المستخدم في الإخفاء و كلمة السر ومفتاح التشفير، وكلا من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً.

بالرغم من الأهمية الكبيرة و الفوائد الجليلة التي يقدمها هذا العلم إلا أن انتشاره حتى هذه اللحظة لا يقارن بانتشار علم التشفير. و القوة التي ينتجها اتحاد هذان العلمان قد تكون قوة لا يستهان بها حيث أن اجتماعهما مع بعضهما البعض يؤدي إلى حصولنا على رسـائل سـرية صـعبة فـي فـك التـشفير وصـعبة فـي إدراك وجودهـا.

تم إنجاز أبحاث كثيرة في مختبر المعالجة الرقمية ومنها: إخفاء المعلومات في صور البصمة الرقمية وإمكانية استخدامها من قبل رجال الدوريات. نمذجة خوارزميات العلامات المائية والمبنية على الترميز الهرمي لإثبات الملكية. إنتاج واختبار طرق جديدة لإخفاء المعلومات ذات سعة عالية جداً مع الحفاظ على كفاءة الحامل

قد يتساءل البعض..وما الحاجة إلى إخفاء وجود البيانات ولم الخوف؟ والسبب يعود إلى وجود حالات قد يكون فيها مجرد وجود شك لدى السلطات أو العصابات أو غيرهم، بتسرب معلومات ما، كفيل بالقضاء على حياة إنسان! كما في حالات انتهاكات السلطات لحقوق الإنسان، وأثناء الحروب الأهلية، أو وللمراسلين والصحفيين الذين يغطون الحروب والغزوات والنزاعات، الـراغبين فـي إيـصال الحقيقـة للعـالم، دون أن يعرضـوا حيـاتهم أو حيـاة غيـرهم للخطـر.

ومثال جيد على هذه الحالات، ما حصل إبان الحرب الأهلية في جواتيمالا، والتي قتل فيها ١٠٠٠٠٠ شخص، فبحسب ما فإن المنظمة العالمية لحقوق الإنسان ((The International Center of1يذكره (Human Rights Research Korhorn) قد جمعت حوالي ٥٠٠٠ شهادة، من شهود عيان، عن طريق استخدام هذه التقنية مع التشفير، فحصلت على المعلومات وحافظت على حيـاة الـشهود.

حاليًا تشغل الأبحاث في مجال هذه التقنية، حيزًا كبيرًا من اهتمام الباحثين، لسبب بسيط وهو أن لها استخدامات هامة في التجارة الإلكترونية، التي تزداد تطبيقاتها، والاهتمام تطبيقاتها العلامات المائية أو ما يعرف بـ بها يومًا بعد آخر. حيث من (Watermarks). وتستخدم هذه الأخيرة في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة، مثل الأسطوانات الخاصة بالموسيقى وغيرها، وكذلك الصور والبرامج التي تباع عبر الإنترنت. فبالرغم من أن المشتري هنا قد يعلم بوجود هذه العلامات، لكنه لا يعرف أين توجد داخل المنتج، ولا البرنامج الذي استخدم في عملية الإخفاء، ولا كلمة السر ومفتاح التـشفير، وبالتـالي يـصعب عليـه، إزالتهـا، وإعـادة النـسخ.

وقد يعد استخدام الستيغانوغرافي في هذا المجال أهم استخداماتها على الإطلاق، وهو أكثر أهمية من استخدامها في مجال الحماية وأمن المعلومات إذ لا يزال التشفير هو سيد الموقف، ولا تزال الستيغانوغرافي هنا ابنة عمه الفقيرة، وإن كانا يستخدمان غالبًا معًا فـي مجـال الحمايـة، حيـث يـتم تـشفير البيانـات أولاً ثـم إخفاؤهـا.

وبالرغم من أن هذه التقنية حديثة نسبيًا إلا أن هناك العديد منها في السوق وعبر الإنترنت، والتي تستهدف المستخدم العادي، والتي تعمل بهذه التقنية

هدف البحث

تسليط الضوء على تقنية اخفاء المعلومات باستخدام العلامة المائية

حدود البحث

يتحدد البحث الحالي بدراسة كيفية الستخدام العلامة المائية في عملية اخفاء البيانات

منهج البحث

يعتمد منهج البحث الحالي على الدراسة النظرية والتحليل العلمي للتعرف على استخدام العلامة المائية في اخفاء البيانات باستخدام الحاسوب .

تحديد المصطلحات

اولا :- اخفاء البيانات (الستيجانوجرافي) هناك عدة تعريفات لتقنية اخفاء المعلومات نذكر منها :-

- تعرف تقنية اخفاء البيانات الستيجانوغرافي **أل (Steganography)بانها فن أخفاء المعلومات بطرق تمنع كشف الرسائل المخفية**
- . الستيغانوغرافي هو إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى، لهدف محدد. والبيانات المستخدمة كظرف أو وعاء للإخفاء يمكن أن تكون عبارة عن ملفات الوسائط المتعددة (الملتيميديا) كالصور، والنصوص، وملفات الصوت أو الفيديو، وغيرها. وقد تكون كذلك ملفات تنفيذية لبرامج مختلفة من نوع (exe). وهكذا في عملية الإخفاء
- يشمل نظام إخفاء المعلومات طرقا لنقل معلومات مضمنة بأسلوب يجعل من الرسالة المرسلة غير مرئية، وربما يكون الحامل لهذه الرسالة ملفا صوتيا أو ملفا نصيا أو صورة.
- هو علم اخفاء البيانات والمعلومات السرية في غطاء رقمي مثل الملفات الصوتية او الصور او ملفات الفديو بحيث يصعب على المشاهد العادي حتى معرفة شيء مخفي .
- هو علم وفن اخفاء البيانات المراد ارسالها (وقد تكون رسائل نصية او صورية) داخل بيانات مرسلة .

_ يستخدم الـ Steganography في اخفاء ملفاتك الهامه داخل ملفات أخرى مثل صورة، فيديو، ملف صوتي، مستند... الفرق بينه وبين التشفير أننا هنا نلجأ لاخفاء المعلومات داخل ملفات أخرى عوضا عـن تـشفيرها. هناك عدة تعاريف أخرى لعلم الإخفاء من أبرزها تعريف العالمين جونسن و جوجوديا على أنه: «فن إخفاء المعلومات بطريقة لا تسمح باكتشافها» .

ثانيا :- العلامة المائية

_ هي احد العلامات التجاريه، وجدت قديما في البدايه في ايطاليا، قد تكون في شكل بعض الحروف مثلا/الحرف الاول من اسم صاحب المصنع او يكتب اسمه بالكامل وقد تكون علي هيئة شكل لصقر او اشكال ادميه او حيوانيه او هندسيه او اشكال خرافيه

_ في العلامة المائية تكون **المادة الرقمية نفسها، أو الملف الرقمي ذاته، هو الهدف من عملية الاتصال والتبادل والحماية، والبيانات المخفية في داخله تصبح جزءًا منه، وتهدف إلى الحفاظ عليه، وتنظيم عملية تبادله**

_ وهي إمكانية وضع خاتم مصدّق كإثبات على أن الصورة تبدو تماماً مثلما كانت عند تصويرها. وستعرف على الفور إذا تغير بكسلاً واحداً من الصورة. وعلى الرغم من أن ميزة العلامة المائية لا تعني الكثير بالنسبة للمستخدم العادي، إلا أنها مهمة جداً بالنسبة للجهات القانونية وشركات التأمين، والمصورين في مجال العلوم والطب.

_ تعرف العلامة المائية على أنها إضافة توقيع صغير أو جزء صغير من البيانات مرئي أو غير مرئي بخوارزم ومفتاح معين إلى الوسط الرقمي بغية تعريف المؤلف أو المالك أو الوسط نفسه أو بغية إضافة معلومات عن الوسط الرقمي كطريقة التشغيل أو العرض المفضلة مثلا كذلك يمكن استخدام هذه العلامات لتعريف البائع أو المشترى لهذه النسخة من الوسط الرقمي , ويشترط لإضافة هذه العلامة ألا تؤثر على جودة الوسط نفسه .

_ العلامة المائية تعني إضافة معلومات معينة إلى الوسط الحامل بحيث لا تؤثر هذه الإضافات على إشارة الحامل إن كان من ناحية الرؤيا إذا كان هذا الوسط عبارة عن معلومات مرئية صورة مثلاً، أو من ناحية السمع إن كان الوسط الحامل عبارة عن معلومات صوتية .

الفصل الثاني

العلامات المائية watermarking

تعتبر هذه العلامات الرقمية من اهم تطبيقات التقنية التي نتحدث عنها واكثرها رواجا واستخداما فاالعلامة الرقمية المائية هي رسالة مخفية داخل صورة رقمية او ملف صوتي او ملف فيديو رقمي او غيرهم من الملفات التي يتم تداولها تجاريا ويتم تخزين هذه الرسالة داخل محتويات الملف ذاته ،فلا تحتاج لمساحة اضافية للتخزين .فالمساحة مهمة جدا ومحدودة .ولذلك فأن هذه الرسالة (العلامة) غالبا ماتكون صغيرة اي تحتوي كميةمحدودة من البيانات .رقما ما غالبا. ويمكن ان تكون هذها العلامة المائية عبارة عن اسم المنتج .اسم الناشر ،بيانات الشركة ، رقم تسلسلي او رقم تعريفي خاص بالمشتري تضمن له حقوقه في ملكية ما اشتراه وتحميه في حالات التحقيق .كما توضح له عدد النسخ المسموح له انتاجها منها وقد اكتسبت العلامة المائية الرقمية هذه اللأهمية . للأنها تسهم في حفظ حقوق الطبع والنشر والتأليف والملكية في العالم الرقمي ،في ظل تزايد عمليات القرصنة والاستنساخ غير المشروع ،خاصة عبر الأنترنيت . ومع تنامي التجارة الألكترونية تزداد الحلجة لتقنية تحفظ هذه الحقوق فغياب وسيلة فعالة حتى الآن في التدقيق والمحاسبة من اجل الحفاظ عبر الملكيات مشكلة كبيرة لهذا النوع من التجارة ، خاصة للأعمال الفنية والموسيقية

تاريخ علم الأخفاء steganography

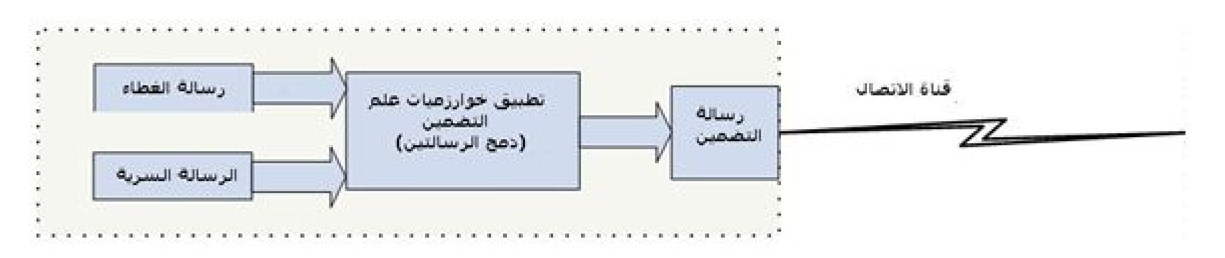
علم الأخفاء لايعد من العلوم المستحدثة .فلقد كان اول ضهور لهذا العلم في العصر الاغريقي ،حيث قام احد رجالات العصربااللتواصل مع احد اقربائه في اليونان ، عن طريق حلق شعر رؤوس عبيده ثم وشم الرسائل على رؤوسهم بعد ذالك يقوم بأنتظار نمو شعر رأسهم ثم ارسالهم الى الشخص الذي يهدف الى التواصل معه ثم جاء بعده العديد من الاشخاص الذين استخدموا الناس والحيوانات واخشب المغطى باالشمع كوسيلة للتواصل مع الناس بطريقة خفية واستمر تواصل هذا العلم ، حتى توصل العالم الى اختراع الحبر الخفي ايان الحرب العالمية الثانية ، والذي ساهم كثيرا في التواصل بين اطراف الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الاسرار وقد تطور علم الاخفاء في الوقت الحالي كثيرا، فأصبح يستخدم المعلومات الرقمية ، والكومبيوترات كوسيلة لنقل البيانات وتذكر كارين كورهورن(Karen korhorn) ان المنظمة العالمية لحقوق الانسان قد جمعت حوالي ٥٠٠٠ شهادة من شهود عيان عن طريق استخدام هذه التقنية مع التشفير فحصلت على المعلومات وحافضات عن حياة الشهود

فن الأخفاء

يأتي اصل مصطلح علم اخفاء المعلومات (steganography)من الكلمتين الاغريقيتين stegos والتي تعني السقف او الغطاء وgraphia والتي تعني الكتابة ويعرف علم الاخفاء على انه اخفاء رسالة ما (بيانات) داخل رسالة اخرى (بيانات اخرى) يهدف اخفاء وجود الرسالة الاولى ،لهدف محدد. والبيانات المستخدمة في الاخفاء قد تكون عبارة عن ملفات الوسائط المتعددة (multimedia) كالنصوص ، الصور وملفات الصوت او الفيديو وغيرها وقد تكون ايضا عبارة عن ملفات تغذية للبرامج (executable file) وفي عملية الاخفاء تحتاج الى توفر عنصرين مهمين لأتمام هذه العملية ، وهناك عدة تعاريف اخرى لعلم الأخفاء من ابرزها تعريف العالمين جونس وجوجوديا على انه ((فن اخفاء المعلومات بطريقة لاتسمح بأكتشافها .

اساليب الاخفاء

يتم إخفاء الرسالة عن طريق إدخالها ضمن الغطاء والذي غالبا ما يكون ملف نصي أو صورة أو ملفات صوت أو فيديو ثم إرسالها إلى الأطراف المعنية. في ما يلي سنقوم بشرح مبسط لكافة أنواع الإخفاء.



صورة ١: طريقة إخفاء المعلومات

الإخفاء النصي

وذلك عن طريق إخفاء الرسالة المراد إرسالها باستخدام النصوص. وتتم هذه الطريقة إما بطريقة نصية، مثلاً: يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفاة. أو بطريقة نحوية أو لفظية. ويعتبر هذا النوع من الإخفاء من أصعب أنواع الإخفاء .

استخدام الحرف الأول من كل كلمة

تعتبر هذه الطريقة من أوائل طرق الإخفاء النصي، و يمكن تطبيقها على اللغة العربية والانجليزية. في هذه الطريقة، يتوجب بناء قطعه نصية مفهومة بحيث عندما يقوم المستقبل بجمع الأحرف الأولى أو الأخيرة مثلا من كل كلمة يحصل على الرسالة السرية. في ما يلي مثال مبسط لهذه الطريقة:

Bring us your invoice by Monday

والتي قد تعني:

BUY IBM

لهذه الطريقة عدة عيوب وهي: السعة المحدودة وعدم وجودة الليونة في تضمين النص السري، حيث يتوجب على المرسل بناء جمل مفهومة في نفس الوقت تحوي على حروف الرسالة السرية.

وهناك عدة طرق أخرى سأقوم بتعدادها فقط: طريقة استخدام نموذج(Tamplet)، طريقة تغيير أماكن التنقيط، طريقة استخدام المد (إطالة الكلمات باستخدام ـ)، طريقة استخدام التشكيل، و طريقة استخدام Texts Unicode. و تعد آخر طريقة من أجدد الطرق المستخدمة في الإخفاء. بالاعتماد على الملاحظة قد يتمكن القارئ من معرفة أن بعضا من هذه الطرق يخص اللغة العربية فحسب.

الإخفاء الصوري

وذلك عن طريق إخفاء الرسالة المراد إرسالها تحت ملف صوري، ويعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء. ويتم تطبيق هذه النوع من الإخفاء باستخدام أحد الطرق التالية: الإخفاء باستخدام التحويل الزاوي المتقطع، الإخفاء باستخدام التحويل الموجي والإخفاء باستخدام الإدخال في البت الأقل أهمية. وتعد طريقة الإدخال في البت الأقل أهمية من أكثر الطرق شيوعاً، وفي ما يلي شرح مبسط لهذه الطريق مع مثال بسيط لتوضيح كيفية عملها.

الإدخال في البت الأقل أهمية

باستخدام هذه الطريقة نقوم باستبدال البت الأقل أهمية من الصورة ببيانات جديدة بطريقة لا تقوم بإحداث الكثير من التغير في الصورة المستخدمة لإرسال الرسالة السرية. من المميزات الأساسية لهذه الطريقة هي أنه بعد القيام بعملية الإخفاء لا يحدث تغيراً يذكر في حجم الغطاء (الملف المستخدم لإخفاء الرسالة السرية). بالرغم من وجود ميزة كهذه في هذه الطريقة إلا أن هناك عيبان رئيسيان قد يعيقان عملية عدم اكتشاف الإخفاء، العيب الأول: هو أن الإخفاء قد يؤثر على جودة الصورة مما قد يؤدي إلى الشك في وجود رسائل مخفاة بها. والعيب الثاني: هو محدودية البيانات التي أستطيع إخفائها في حيز الصورة. في الأسفل مثال توضيحي:

لإخفاء الحرف "a" (ASCII code 97, that is ٠١١٠٠٠٠١) داخل صوره (غطاء) حجمها ثمانية بايت ، نقوم بتحويل البت الأقل أهمية في كل بايت إلى بت من الحرف المراد إخفاؤه.

١٠٠١٠٠١٠
٠١٠١٠٠١١
١٠٠١١٠١١
١١٠١٠٠١٠
١٠٠٠١٠١٠
٠٠٠٠٠٠١٠
٠١١١٠٠١٠
٠٠١٠١٠١١

ثم نقوم بإرسالها للمستقبل، ويقوم هو بدوره باستخراج الملفات المخفاة. وهناك برامج تتواجد على الانترنت بعضها يمكن تحميله واستخدامه مجانا، وتقوم هذه البرامج بعملية إخفاء البيانات المرغوبة بالصور التي يختارها المستخدم.

الإخفاء الفيديوي

يعتبر الإخفاء باستخدام ملفات الفيديو جزءا مشتقاً من الإخفاء باستخدام الصور، وذلك لأن ملفات الفيديو عبارة عن صور مجتمعة، لأجل هذا تقنيات الإخفاء بالصور يمكن استخدامها في هذه الطريقة. ومن أشهر الطرق المستخدمة في هذا النوع طريقة الإخفاء باستخدام التحويل الزاوي المتقطع (Cosine Transform Discrete). وتقوم هذه الطريقة بإخفاء جزء من المعلومات في جزء معين من الصور التي يتكون منها الفيديو، وتمتاز هذه الطريقة بأنها غالبا لا يتم اكتشاف البيانات المخفاة بالفيديو باستخدام العين البشرية. لكن يجب ملاحظة أنه كلما ازداد حجم البيانات المخفاة كلما كان كشفها أسهل في جميع الطرق المستخدمة للإخفاء.

الإخفاء الصوتي

ويتم في هذه الطريقة إخفاء الرسالة المراد إرسالها داخل إشارة صوتية ممكن أن تكون في مجال الزمن أو مجال الطيف. ويتم بإحدى الطرق التالية :

تغطية الإدراك

وتعد هذه الطريقة من أكبر الطرق المستخدمة من ناحية سعة الإدخال(٤٥٠،٠٠٠ بت في الثانية) لكنها من أضعف الطرق في الإخفاء ، حيث تعد من أكثر الطرق عرضة للاكتشاف. ترميز البت المنخفض

وتمتاز هذه الطريقة بسعة إدخال عالية (٤١،٠٠٠ بت في الثانية) لكنها عرضة للاكتشاف من قبل المهاجمين. وفي هذه الطريقة يتم إبدال أكثر بت غير مهم (Least Significant Bit) من كل إشارة صوتية ، وتقنية هذه الطريقة مشابهة جداً لتقنية إبدال أكثر بت غير مهم في الإخفاء الصوري الطيف الممتد

ويتم في هذه الطريقة إدخال الرسالة داخل الترددات العالية. وتعتبر أكثر طريقة من ناحية الإخفاء لكن سعة الإدخال فيها منخفضة جداً (٤ بت في الثانية)، بالرغم من سعتها المنخفضة إلا أنها من أقوى الطرق حماية للمعلومات المخفاة حيث أن الأذن البشرية لا تستطيع تميز الاختلاف بالصوت بخلاف الطريقتين السابقتين والتي يمكن للإذن البشرية تمييز التشويش في الصوت الناتج عن عملية الإخفاء.

الخلاصة

بالرغم من الأهمية الكبيرة و الفوائد الجليلة التي يقدمها هذا العلم إلا أن انتشاره حتى هذه اللحظة لا يقارن بانتشار علم التشفير. وكما سبق وأن أوردت القوة التي ينتجها اتحاد هذان العلمان قد تكون قوة لا يستهان بها حيث أن اجتماعهما مع بعضهما البعض يؤدي إلى حصولنا على رسائل سرية صعبة في فك التشفير وصعبة في إدراك وجوده.

خلاصة للبحوث التي قمت بها لإنتاج هذا المقال، وجدت قلة في المصادر العربية التي تهتم بهذا العلم وبغير من علوم أمن المعلومات ، وبالرغم من الحاجة الماسة في مجتمعنا العربي لباحثين مهتمين بهذا العلم إلا إنّي لم أجد غير باحثين من جامعتين مختلفتين قاما معاً بإيجاد بعض الطرق المستحدثة لاستخدامها في إخفاء المعلومات باللغة العربية. أتمنى أن يكون هذا المقال بذرة من البذرات الأولية التي تحفز المهتمين بعلوم حماية المعلومات إلى الانطلاق الحثيث سعياً وراء تطوير هذا العلم واستخدامه بقوة في لغتنا العربية.

ما هو التشفير أو التعمية (Cryptography):

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكّنك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنه- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل اي شخص ما عدا الشخص المرسل لـه. وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (Cryptoanalysis) هو علم لكسر و خرق الاتصالات الآمنة.

أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

١- السرية أو الخصوصية (**Confidentiality**):

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

٢- تكامل البيانات (**Integrity**):

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

٣- إثبات الهوية (**Authentication**):

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

٤- عدم الجحود (**Non-repudiation**):

وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

كيفية عمل التشفير:

خوارزمية التشفير هو دالة رياضية تستخدم في عملية التشفير وفك التشفير. وهو يعمل بالاتحاد مع المفتاح أو كلمة السر أو الرقم أو العبارة، لتشفير النصوص المقروءة.

نفس النص المقروء يشفر إلى نصوص مشفرة مختلفة مع مفاتيح مختلفة. والأمن في البيانات المشفرة يعتمد على أمرين مهمين قوة خوارزمية التشفير وسرية المفتاح. فيما يلي رسم توضيحي صورة(١).



صورة١: طريقة عمل التشفير

أنواع التشفير:

حالياً يوجد نوعان من التشفير وهما كالتالي:

١- التشفير التقليدي (**Conventional Cryptography**).

٢- تشفير المفتاح العام (**Public Key Cryptography**).

التشفير التقليدي:

يسمى أيضاً التشفير المتماثل (Symmetric Cryptography). وهو يستخدم مفتاح واحد لعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. مثال على ذلك؛ إذا أراد زيد إرسال رسالة مشفرة إلى عبيد، عليه إيجاد طريقة آمنة لإرسال المفتاح إلى عبيد. فإذا حصل أي شخص ثالث على هذا المفتاح فإن بإمكانه قراءة جميع الرسائل المشفرة بين زيد وعبيد. فيما يلي رسم توضيحي صورة (٢).



صورة٢: توضح عمل التشفير باستخدام المفتاح الواحد

بعض الأمثلة على أنظمة التشفير التقليدي:

- **شيفرة قيصر:** وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها. المثال التالي يوضح طريقة عمل شيفرة قيصر: إذا شفرنا كلمة **"SECRET"** واستخدمنا قيمة المفتاح ٣، فإننا نقوم بتغيير مواضع الحروف ابتداءً من الحرف الثالث وهو الحرف **"D"**، وعليه فان ترتيب الحروف سوف يكون على الشكل التالي:

ZA B C D E F G H I J K L M N O P Q R S T U V W X Y

الحروف بعد استخدام القيمة الجديدة لها من المفتاح "٣" تكون على الشكل الحالي:

CD E F G H I J K L M N O P Q R S T U V W X Y Z A B

الآن قيمة الـ **A** **à** **D**، **B** **à** **E**، **C** **à** **F**، وهكذا.

بهذا الشكل فان كلمة **"SECRET"** سوف تكون **"VHFUHW"**. لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة؛ يجب أن ترسل له قيمة المفتاح **"٣"**.

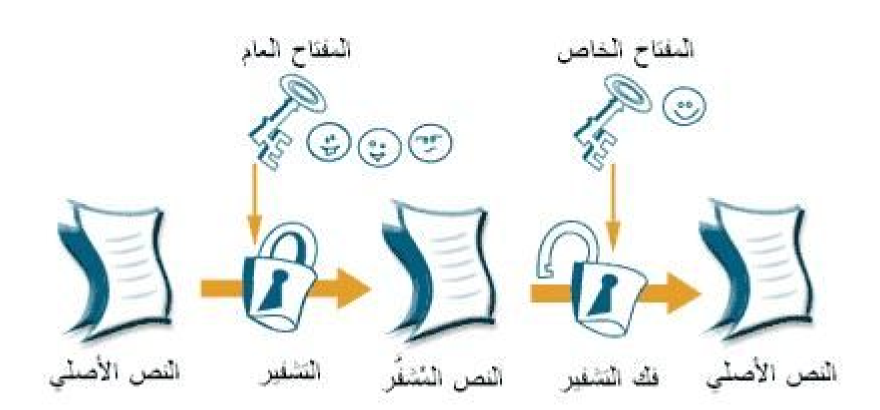
- **تشفير البيانات القياسي (DES):** طُور هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الكمبيوتر وزيادة سرعة معالجته للبيانات، حيث أنه قد يتم كشف محتوى رسائل مشفرة به في وقت قصير.

- **AES, IDEA, 3DES, blowfish**،: وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير.

كل ما ذكر من الأمثلة السابقة يعتمد على مبدأ المفتاح الواحد لعملية التشفير وفك التشفير.

تشفير المفتاح العام:

أو ما يعرف بالتشفير اللامتماثل (Asymmetric Cryptography). تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاص Privet key، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص. فيما يلي رسم توضيحي صورة (٣).



صورة٣: توضح عمل التشفير باستخدام المفتاح العام والمفتاح الخاص

بعض الأمثلة على أنظمة تشفير المفتاح العام:
RSA, Elgamal, Deffie-Hellman, DSA, PGP,

جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص.

مزايا وعيوب التشفير التقليدي والتشفير باستخدام المفتاح العام:

التشفير التقليدي أسرع بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه يستخدم مفتاح واحد فقط. فهو عرضة أكثر للاختراقات. أما تشفير المفتاح العام فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة للاختراقات، ولكنه أبطأ من التشفير

التقليدي.

ونتيجة لهذه المزايا والعيوب أصبحت الأنظمة الحديثة تستخدم كلا الطريقتين حيث أنها تستخدم الطريقة التقليدية للتشفير وأما تبادل المفتاح السري الواحد بين الأطراف المتراسلة تتم من خلال استخدام طريقة تشفير المفتاح العام.

قياس قوة التشفير:

التشفير قد يكون قوياً أو ضعيفاً، حيث أن مقياس القوة للتشفير هو الوقت والمصادر المتطلبة لعملية كشف النصوص غير مشفرة من النصوص المشفرة. نتيجة التشفير القوي هو نص مشفر يصعب كشفه مع الوقت أو توفر الأدوات اللازمة لذلك.

خاتمة:

فائدة التشفير كبيرة، حيث انه يوفر الخصوصية والأمن بجميع مفاهيمه للبيانات المنقولة عبر الشبكات المفتوحة. فقد باتت الحاجة ملحة لطرق تشفير قوية لأنه مع التطور السريع للكمبيوتر فانه ينقص من قوة التشفير؛ وذلك لان زيادة سرعة الكمبيوتر تعني تقصير الوقت الذي يحتاجه الكمبيوتر لكسر أو كشف مفتاح تشفير معين.

الفصل الثالث

الفرق بين علم التشفير وعلم الإخفاء

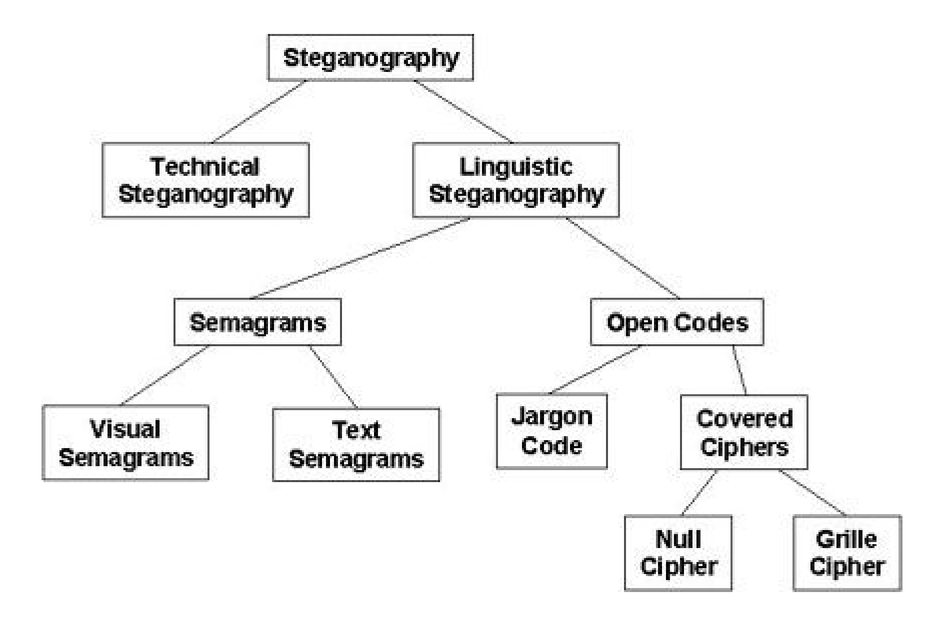
لاكتشاف أهم فرق بين علم التشفير وعلم الإخفاء نكتفي بعرض تعريف لكليهما. فعلم التشفير هو العلم الذي يهدف إلى دراسة طرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل. بينما علم الإخفاء هو العلم الذي يهدف إلى إخفاء وجود الرسالة. إذن الفرق الأساسي هو أن التشفير يغير من هيئة محتوى الرسالة بحيث لا يستطيع أحد قراءتها سوى الأطراف المعنية بها، لكنه لا يخفي وجودها. أما علم الإخفاء فيخفي محتوى الرسالة في المقام الأول. في الأسفل سنقوم بعرض مقارنة بينهما في النواحي الأخرى

	علم التشفير	علم الإخفاء
من حيث العلم بوجود الرسالة	يعلم وجود الرسالة	لا يعلم وجود الرسالة
من حيث الاتصال	يمنع الأطراف الآخرين من معرفة محتوى الاتصال	يمنع الآخرين من معرفة وجود الاتصال
من حيث الشيوع	تقنية شائعة	تقنية غير شائعة

جدول ١: مقارنة بين علم التشفير وعلم الإخفاء

علم التشفير وعلم الإخفاء هما طريقتان لحماية المعلومات من عرضها والعبث بها من قبل الأشخاص الغير مرغوبين، لكن كلا من الطريقتين لو استخدمت لوحدها، قد لا تعتبر وسيلة حماية كافية وكاملة. بالنسبة لإخفاء المعلومات مثلا، حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما، فإن الهدف من عملية الإخفاء يصبح بلا قيمة! لذا فإنه ولزيادة حماية المعلومات المخفاة يجب علينا استخدام كلا من تقنيات حماية المعلومات ، التشفير و الإخفاء.

علم اخفاء المعلومات الرقمية – Steganography



المصدر/أبجدية التقنية

خلال السنوات الماضية، أصبح علم أمن المعلومات هو محل اهتمام لكثير من الباحثين التي تحاول جهودهم أن تتوصل إلى حلول وتقنيات و أفكار جديدة تضمن نقل المعلومات بأمان من خلال الشبكة وخاصة شبكة الانترنت دون حدوث أي اختراق وكشف لتلك المعلومات. ونتيجة لذلك، يوجد العديد من التقنيات والأساليب التي تستخدم حالياً في أمن المعلومات. في هذا المقال سنلقي الضوء على طريق جديد نوعا ما لحماية المعلومات، وهو علم التضمين (Steganography)

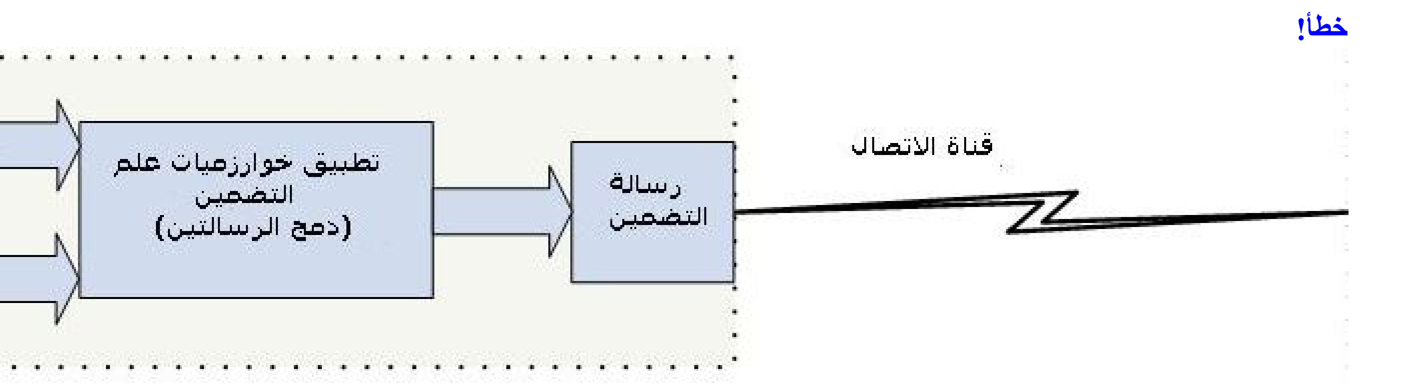
ما هو Steganography ؟

بالحقيقة يصعب تعريف هذا المصطلح باللغة العربية بشكل يغطي معناه الكامل، ولكني سأحاول أن أشرحه بشكل مبسط. ترجع أصل كلمة " Steganography " إلى اللغة اليونانية وتعني "يغطي" أو "يُخفي"،وسأعرفه هنا كمصطلح حاسوبي:

"**علم التضمين** هو العلم الذي يهتم باخفاء المعلومات الرقمية داخل وسيط الكتروني دون احداث أي تشويه أو تعديل ملحوظ في هذا الوسيط"

لنبدأ ونشرح هذا التعريف قليلا باعطاء مزيداً من التوضيح لكي يسهل فهم الفكرة العامة. لنقل لديك معلومات أو ملفات رقمية (نص، صورة، صوت) تريد ارسالها عبر الشبكة لكي تصل بشكل آمن إلى الطرف الآخر، ودعونا نطلق على تلك المعلومات والملفات **بالرسالة السرية**. الرسالة السرية لن تُرسل بشكل مباشر ولكن يجب أن تدمج وتكون مخفية داخل **رسالة الغطاء** (أيضاً هذه الرسالة قد تكون نص، صورة، صوت) بشكل احترافي دون ترك أي أثر أو شك بأن هناك رسالة سرية داخل رسالة الغطاء. وبالتالي تكون ناتج عملية الدمج هي **رسالة التضمين** والتي هي عبارة عن نسخة من رسالة الغطاء من حيث الشكل ولكنها تحتوي الرسالة السرية دون احداث أي شك أو ريب بوجودها.

خطأ!



لتوضيح الصورة أكثر، دعونا نتخيل هذا المشهد:

أمجد وكامل في سجن منفصل، يريدان أن يتخاطبا لعمل خطة لهروب من السجن الذي يأسا منه. جميل سوف يسمح لهم بالمخاطبة بشرط أنه سيراقب هذا الاتصال، فما الحل ؟

الحل هو البحث عن طريقة تسمح لهم بالاتصال على أن يظهر هذا الاتصال بشكل بريئ غير مشبوه للشخص الذي يراقب، دون علمه بحقيقة ما يجري وراء هذا الاتصال. وهذا هو فكرة عمل علم التضمين. ارسال رسائل تظهر بشكل بريئ دون علم المستخدم العادي بوجود معلومات سرية مخبئة داخل تلك الرسائل.

:

ألـــــــــــــــــــستيغانوغرافي(steganography)

تهدف تقنية الستيغانوغرافي (Steganography)إلى إخفاء البيانات داخل بيانات أخرى، بطريقة لا تؤدي إلى التأثير في هذه الأخيرة، بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف الحقيقة. والغرض من عملية الإخفاء هذه ألا يعلم المهاجم المحتمل عن وجود هذه البيانات، وبالتالي يتم حمايتها من القراءة أو التغيير أو التدمير عن طريق هذا المهاجم، لأنه إذا كنت لا تعلم بوجود شيء ما أصلاً فكيف يمكن لك الاستفادة منه أو تدميره؟ وهذا الذي يجعل هذه التقنية مختلفة عن التشفير (Cryptography)، ففي التشفير يعلم المهاجم بوجود هذه البيانات، وقد يستطيع الوصول إليها، لكنه لا يستطيع قراءتها إلا بعد كسر الشفرة، لكنه قادر على إزالتها إذا شك فيها مثلاً.

قد يتساءل البعض..وما الحاجة إلى إخفاء وجود البيانات ولم الخوف؟ والسبب يعود إلى وجود حالات قد يكون فيها مجرد وجود شك لدى السلطات أو العصابات أو غيرهم، بتسرب معلومات ما، كفيل بالقضاء على حياة إنسان! كما في حالات انتهاكات السلطات لحقوق الإنسان، وأثناء الحروب الأهلية، أو وللمراسلين والصحفيين الذين يغطون الحروب والغزوات والنزاعات، الراغبين في إيصال الحقيقة للعالم، دون أن يعرضوا حياتهم أو حياة غيرهم للخطر. ومثال جيد على هذه الحالات، ما حصل إبان الحرب الأهلية في جواتيمالا، والتي قتل فيها ١٠٠٠٠٠ شخص، فبحسب ما فإن المنظمة العالمية لحقوق الإنسان ((The International Center of1يذكره Human Rights Korhorn) Research) قد جمعت حوالي ٥٠٠٠ شهادة، من شهود عيان، عن طريق استخدام هذه التقنية مع التشفير، فحصلت على المعلومات وحافظت على حياة الشهود.
حاليًا تشغل الأبحاث في مجال هذه التقنية، حيزًا كبيرًا من اهتمام الباحثين، لسبب بسيط وهو أن لها استخدامات هامة في التجارة الإلكترونية، التي تزداد تطبيقاتها، والاهتمام تطبيقاتها العلامات المائية أو ما يعرف بـ بها يومًا بعد آخر. حيث من (Watermarks). وتستخدم هذه الأخيرة في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة، مثل

الأسطوانات الخاصة بالموسيقى وغيرها، وكذلك الصور والبرامج التي تباع عبر الإنترنت. فبالرغم من أن المشتري هنا قد يعلم بوجود هذه العلامات، لكنه لا يعرف أين توجد داخل المنتج، ولا البرنامج الذي استخدم في عملية الإخفاء، ولا كلمة السر ومفتاح التشفير، وبالتالي يصعب عليه، إزالتها، وإعادة النسخ.
وقد يعد استخدام الستيغانوغرافي في هذا المجال أهم استخداماتها على الإطلاق، وهو أكثر أهمية من استخدامها في مجال الحماية وأمن المعلومات إذ لا يزال التشفير هو سيد الموقف، ولا تزال الستيغانوغرافي هنا ابنة عمه الفقيرة، وإن كانا يستخدمان غالبًا معًا في مجال الحماية، حيث يتم تشفير البيانات أولاً ثم إخفاؤها.
وبالرغم من أن هذه التقنية حديثة نسبيًا إلا أن هناك العديد منها في السوق وعبر الإنترنت، والتي تستهدف المستخدم العادي، والتي تعمل بهذه التقنية. وأذكر هنا برنامجين قمت Suit). Security بتجربتهما: وهما (Hiderman) و(Steganos
ما هو الستيغانوغرافي Steganography؟
الستيغانوغرافي هو إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى، لهدف محدد. والبيانات المستخدمة كظرف أو وعاء للإخفاء يمكن أن تكون عبارة عن ملفات الوسائط المتعددة (الملتيميديا) كالصور، والنصوص، وملفات الصوت أو الفيديو، وغيرها. وقد تكون كذلك ملفات تنفيذية لبرامج مختلفة من نوع (exe). وهكذا في عملية الإخفاء هذه نحتاج إلى ملفين أحدهما ، والآخر هو المادة المراد إخفاؤها.)cover(يسمى الغطاء)Jojodiaويُعَرفها &على أنها «فن إخفاء المعلومات بطريقة لا تسمح Johnson 8991(2 باكتشافها».
وكما سبق الذكر فإن ميزته على التشفير في أنه يخفي وجود الرسالة في حين أن الأول يثبت وجودها ولكنها غير مقروءة، وهناك حالات لن يجدي فيها التشفير نفعًا، فإذا ما وقع شخص تحت التعذيب، فسيجبر على فك الشفرة، بينما لا يمكن أن يجبر : «إن)Kuhn 5991(3على فك شفرة شيء غير موجود، أو غير معلوم وجوده أصلاً. يقول الهدف الرئيسي من هذه التقنية هو إخفاء الرسالة السرية، داخل رسالة عادية، بطريقة تجعل العدو غير قادر على اكتشاف وجود رسالة سرية أصلاً».
من أين جاءت هذه التسمية المعقدة (Steganography)؟
الكلمة أصلها يوناني، وهي تعني الكتابة (Covered writing). والستيغانوغرافي كفكرة قديمة قدم التاريخ الإنساني4 4المخفية ذاته. فقدماء الإغريق اعتادوا مثلاً حفر الرسالة السرية على طاولات من الخشب، ثم يغطونها بطبقه من الشمع. وحين تصل الرسالة على الشخص المقصود، يقوم بإزالة أو إذابة الشمع ليحصل على رسالته. كذلك استخدم الإغريق وسيلة أخرى لنفس الغرض، وإن كانت وحشية بعض الشيء، بمقاييس عصرنا بالطبع. حيث كانوا يقومون بحلق رؤوس العبيد، ثم يتم (وشم) الرسالة السرية على هذه الرؤوس البائسة. بعدها يحبسون الشخص حتى يطول شعره، فيغطي فروة رأسه (والرسالة السرية معها)، ويرسلونه إلى الطرف الآخر. وحين يصل إلى هناك، يقوم هذا الأخير بحلق رأس العبد، ويقرأ الرسالة. وفي العصر الحديث كان الحبر السري أحد أهم أدوات العملاء والمخبرين خلال الحرب العالمية الثانية.
وفي العالم الرقمي، يتم إخفاء أي نوع من البيانات والملفات، داخل أنواع عديدة ومختلفة من الملفات. كما أن أحد التطبيقات التي ظهرت نتيجة لهذه التقنية، هي إنشاء حيز داخل القرص الصلب، يُفعّل تلقائيا عند تشغيل الجهاز ويستخدم لتخزين)Partition(المعلومات المراد إخفاؤها.
تحليل الستيغانو Steganalysis:
تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية، أو قراءتها، أو تغيرها أو Steganalysis.
ولنجاح هذه العملية فلابد من أمرين، أولاً: اكتشاف وجود حذفها بـ معلومات مخفية، وثانيًا: تغييرها، أو حذفها أو مجرد قراءتها. وكل وظيفة تقنيتنا هنا هو محاولة إخفاء البيانات بطريقة لا تثير الشبهات، أي لا تترك علامات أو أثرًا يدل على حدوث تغير ما. فمثلا في حالة الإخفاء داخل الصور، يجب مراعاة عدة عوامل منها: عدم استخدام صور معروفة، أو نماذج من صور يمكن لأي شخص الحصول على نسخ منها (مثل صور الإنترنت) للإخفاء حيث تسهل المقارنة في حالة وجود صورتين. وكذلك مراعاة ألا يحدث تغير ظاهر في الصور كتشوهها، أو تغير ألوانها بشكل واضح. ولهذا يُنصح بعدم إخفاء بيانات كثيرة في ذات الصورة خوفًا من تغيير هيئتها، بطريقة تهدم الهدف الأساسي من استخدام التقنية، لأن إثارة الشبهة تعني فشل العملية.
من الصعب التعرف على المادة المخفاة إذا كان البرنامج المستخدم في ذلك مجهولاً للعدو، لكن للأسف بعض البرامج تخفي المعلومات ولكن بطريقة تترك أثرًا يعمل وكأنه مذياع يذيع خبر السر! ولذلك يجب الانتباه عند اختيار برنامج ما لاستخدامه في عملية الإخفاء هذه.
العلامة المائية الرقمية (Digital Water Mark):
تعتبر هذه العلامات الرقمية من أهم تطبيقات التقنية التي نتحدث عنها، وأكثرها رواجًا واستخدامًا. فالعلامة الرقمية المائية، هي رسالة مخفية داخل صورة رقمية، أو ملف صوتي، أو ملف فيديو رقمي أو غيرها من الملفات الرقمية التي يتم تداولها تجاريًا.
ويتم تخزين هذه الرسالة داخل محتويات الملف ذاته، فلا تحتاج لمساحة إضافية للتخزين. فالمساحة مهمة جدًا ومحدودة، ولذلك فإن هذه الرسالة (العلامة) غالبًا ما تكون صغيرة، أي تحوي كمية محدودة من البيانات، رقمًا ما غالبًا. ويمكن أن تكون هذه العلامة المائية عبارة عن اسم المنتج، اسم الناشر، بيانات الشركة، رقم تسلسلي، أو رقم تعريف خاص بالمشتري تضمن له حقوقه في ملكية ما اشتراه وتحميه في حالات التحقيق. كما قد توضح له عدد النسخ المسموح له إنتاجها منها.
وقد اكتسبت العلامة المائية الرقمية هذه الأهمية، لأنها تسهم في حفظ حقوق الطبع والنشر والتأليف والملكية في العالم الرقمي، في ظل تزايد عمليات القرصنة والاستنساخ غير المشروع، خاصة عبر الإنترنت. ومع تنامي التجارة الإلكترونية، تزداد الحاجة لتقنية تحفظ هذه الحقوق، فغياب وسيلة فعّالة حتى الآن في التدقيق والمحاسبة من أجل الحفاظ عبر الملكيات، مشكلة كبيرة لهذا

النـــــــوع مـــــــن التجــــــــارة، خاصـــــــــة للأعمـــــــــال الفنيـــــــــة والموســـــــــــيقية.
الفرق الرئيسي ما بين الستيغانوغرافي التقليدية وما بين العلامة المائية، أنه في الحالة الأولى يتم إخفاء البيانات، حيث تكون هذه البيانات هي الهدف من عملية الاتصال والتبادل، وهي التي يراد حمايتها. بينما في الحالة الثانية، فإن المادة الرقمية نفسها، أو الملف الرقمي ذاته، هو الهدف من عملية الاتصال والتبادل والحماية، والبيانات المخفية في داخله تصبح جزءًا منه، وتهدف إلى الحفاظ عليه، وتنظيم عملية تبادله. ففي الحالة الأولى إذن إخفاء سر وجود المعلومات هو الغاية، ويصبح هدف العدو اكتشاف وجود هذه المعلومات من الأساس. بينما في الحالة الثانية لا يضير أن يعرف أحد بوجود هذه المعلومات، وقراءتهـــا، وإنمـــا هـــدف العـــدو ســـيكون حـــذف هـــذه المعلومـــات أو تغييرهـــا لمـــصلحته.
القاعــــــــــــــــــــــــــــــــــــدة وإســـــــــــــــــــــــــــــــــــــــرائيل:
ملاحظة عابرة من أحد الأشخاص أثارت اهتمامي لأول مرة بالموضوع. وعندما بدأت البحث اكتشفت أن السياسة تطل برأسها كثيـــــــــــــرًا فــــــــــــي هــــــــــــذا الموضــــــــــــوع ولا عجـــــــــــب!
الغريب أنه في أمريكا هناك من يعتقدون أن تنظيم القاعدة يستخدم هذه التقنية الحديثة في . وأن5)Pornography(تبادل الرسائل عبر الإنترنت عن طريق استخدام الصور الفاضحة تبادل المعلومات حول العمليات الإرهابية يتم عبر المواقع الإباحية، ويـــــذهب آخـــــرون إلـــــى أنـــــه ربمـــــا كـــــان لهـــــا دور فـــــي أحـــــداث ســـــبتمبر.
أمر آخر أثار اهتمامي وحسرتي في آن بن واحد، وهو أن الجامعات الإسرائيلية نشطة جدًا في هذا المجال، ومنها جامعة بل يبدو أن الإسرائيليين يتقدمون على الأوروبيين6(University Gurion Ben) غوريون والأمريكيين، بأبحاث تحاول أن تجعل حتى الصور المطبوعة تحتفظ بالمعلومات. ويتم قراءتها باستخدام أجهزة خاصة بطريقة تشبه تلك المستخدمة في محلات الـــــــــــــسوبر ماركـــــــــــــت لقـــــــــــــراءة ســـــــــــــعر الـــــــــــــصنف.
خاتمـــة:
مجال أمن المعلومات ليس مجالاً هامشيًا ولا سهلاً، وله استخدامات قصوى في الحروب بكل أنواعها، والجاسوسية، وغيرها من ألعاب الحرب الباردة أو الساخنة، ونظرًا لأن قرننا هذا يبدو أنه قرن الحروب، فستزداد الحاجة لمثل هذه التقنيات والتطبيقات. وأنا أتساءل هنا عما إذا كنا كعرب ومسلمين مستعدين للدخول في الميدان، متعلمين من غيرنا أولاً، ومشاركين معهم ثانيًا، ومبتكرين متقدمين عليهم ثالثا. فهذه الأمور لا تحتاج إلى ميزانيات ضخمة، ومعامل حديثة، بقدر ما تحتاج إلى عقل واع، وعزيمة، وإرادة على مستوى الشعوب والحكومات، فهل نحن قادرون على التحدي، أو على الأقل كسب شرف المحاولة، خاصة أن العدو المباشر الذي على أبوابنا، ليس نائمًا بل يعمل بخبث لكن باجتهاد وتنظيم وتخطيط لدرجة تثير الإعجاب!

ما الفرق بين Steganography و Cryptography (التشفير) ؟

هناك فرق كبير بين تضمين المعلومات وتشفيرها، ففي الأول المعلومات تكون مخفيه بحيث المستخدم العادي لن يكون على معرفة وعلم بوجود تلك المعلومات، أما في التشفير فأن المستخدم يكون على علم بان هناك معلومة مخفية ولكنها مشفرة غير مفهومة. ولذا فإن أنسب طريقة لبناء نظام حماية قوي، هو الاعتماد على التقنيتين لجعل عملية اختراق النظام أكثر تعقيداً.

تطبيقات علم التضمين:

لهذا العلم الرائع العديد من التطبيقات التي تختلف على حسب نوع التضمين المستخدم (سوف نتحدث عن الأنواع في القسم التالي)، ولكن دعوني أستعرض هنا بعض تلك التطبيقات بشكل عام:

أهم تطبيق هو تبادل المعلومات بشكل آمن دون احداث اي شك للطرف الثالث، وهذا ما قد تم استخدامه في الحروب بين الدول كالحرب العالمية الثانية حيث يتم تبادل الرسائل بين الجيش بطريقة تظهر على أنها عادية للجيش العدو ولكنها تحمل معناً آخر لا يفهمه إلا من هو في نفس الجيش. أو ما يستخدمه الجواسيس لارسال رسائلهم دون احداث شك في الكلام المكتوب.

ومن التطبيقات أيضاً حماية الحقوق الملكية أو الفكرية لجميع انواع الملفات الالكترونية، فعن طريق استخدام العلامة المائية (*Watermarking*) تستطيع أن تثبت بأنك المالك الرسمي للصورة أو ملف الصوت أو الفيديو.

العلامة المائية تعني إضافة معلومات معينة إلى الوسط الحامل بحيث لا تؤثر هذه الإضافات على إشارة الحامل إن كان من ناحية الرؤيا إذا كان هذا الوسط عبارة عن معلومات مرئية صورة مثلاً، أو من ناحية السمع إن كان الوسط الحامل عبارة عن معلومات صوتية. مع انتشار الوسائط المتعددة الرقمية أصبح استخدام العلامات المائية شائع كثيراً، فيمكن أن تستخدم مثلاً لإضافة علامة معينة إلى مجموعة من الصور التي سيتم نشرها عبر موقع ما على الانترنيت و تدل هذه العلامة على مالك هذه الصور و ذلك لحماية حقوق الطبع و النشر لهذا المالك، فمن يريد أن ينسخ تلك الصور لن يعلم أن هناك علامة معينة أضيفت لتلك الصور و يمكن أن تفضح أمره إن ادعى أن هذه الصور له. (ويكيبيديا)

أنواع التضمين (Steganography) :

أرجو ان تكون قد هضمت الفكرة العامة للتضمين والتي هي أساسها اخفاء المعلومات لا غير! يعتمد اخفاء المعلومات على الوسط المتسخدم (رسالة الغطاء) الذي بدوره سيحدد نوع التضمين المستخدم. و من أبرز تلك الأنواع:

١- اخفاء المعلومات في النصوص (التضمين النصي)

٢- اخفاء المعلومات في الصور (التضمين باستخدام الصور)

٣- اخفاء المعلومات في الصوت و الفيديو

التضمين النصي يعتبر من أصعب الطرق لاخفاء المعلومات، اما التضمين باستخدام الصور فهو النوع الأكثر شيوعاً لما تحمل الصور من صفات تجعلها الوسط المثالي للتضمين.

التضمين النصي هو النوع المفضل لدي لما فيه من تحديات وصعوبات في تضمين الرسالة التي يراد اخفاؤها. بلاشك هذا النوع هو أصعب أنواع التضمين وذلك لصعوبة وجود بينات زائدة (redundant bits) يمكن استغلالها و استبدالها بالرسالة السرية، أيضاً تعديل النصوص يختلف عن الصور حيث سيكون من السهل ملاحظة أي تعديل يطرأ على الكلمات المكتوبة.

يوجد عدة خوارزميات مهتمة بالتضمين النصي، وتختلف من لغة إلى لغة. فمثلاً، طرق التضمين في اللغة العربية ليست بالضرورة أن تكون قابلة للتطبيق على جمل اللغة الانجليزية، والعكس صحيح، لذا قد يستفاد من التنقيط الموجود في أحرف اللغة العربية في تضمين النصوص المراد اخفاؤها، وكما هو معلوم أن حروف العربية غنية بالنقاط، بل من الصعب أن تجد كلمة عربية بدون تنقيط، مقارنة باللغة الانجليزية، فلا يوجد سوى حرفين بهما نقاط هما: [i، j] !!

كما ذكرت سابقا، هذا النوع صعب جداً وبالكاد أن تجد بحوثا مهتمة بهذا الشأن بشكل عام، ولكن، بالرغم من صعوبته والتحديات التي ستواجه الباحثين، يوجد عددا لا بأس به من البحوث التي اهتمت بهذا الشأن في اللغة العربية، وكانت جامعة الملك فهد للبترول والمعادن أحد الجامعات التي قدمت طرقاً جديرة بالاطلاع عليها، أيضاً هناك جامعة أخرى في إيران التي كان لها دور مهماً في تقديم طرق جديدة للتضمين النصي.

وقبل الخوض في تفاصيل طرق التضمين، يجب أن لا ننسى الهدف من التضمين، و هو اخفاء المعلومات السرية دون ترك أثر أو جلب الشك في الرسالة النهائية (رسالة التضمين).

سأبدأ ببعض الطرق البسيطة التي يمكن تطبيقها بدون أدوات أو برامج، ومن ثم سأنتقل إلى الطرق المتقدمة والتي قد تحتاج أدوات خارجية وبرامج إلى تطبيقها:

- **الحرف الأول من كل كلمة:**

تعتبر من أوائل طرق التضمين النصي، يمكن تطبيقها على اللغة العربية والانجليزية، في هذه الطريقة، يجب بناء قطعه مفهومة بحيث اذا جمعت الأحرف الأولى (أو الأخيرة حسب اختيارك) من كل كلمة تخرج بالرسالة السرية، اليك هذا المثال:

your invoice by Monday Bring us

والتي قد تعني:

IBM BUY

مايعيب هذه الطريقة هو السعه المحدودة وعدم وجودة الليونة في تضمين النص السري بحيث عليك بناء جمل مفهومة وبنفس الوقت اختيار كلمات تحمل حروف الرسالة السرية.

- **استخدام نموذج (Template) :**

أحد الطرق الأخرى للتضمين هي استخدام نموذج جاهز (قطعة جاهزة) تحوي على فراغات، ثم عليك بتعبئة الفراغات بكلمات الرسالة السرية، اليكم هذا المثال:

THE MOST COMMON WORK ANIMAL IS THE HORSE. THEY CAN BE USED

TO FERRY EQUIPMENT TO AND FROM WORKERS OR TO PULL A PLOW.

BE CAREFUL, THOUGH, BECAUSE SOME HAVE SANK UP TO THEIR

KNEES IN MUD OR SAND, SUCH AS AN INCIDENT AT THE BURLINGTON

FACTORY LAST YEAR. BUT HORSES REMAIN A SIGNIFICANT FIND. ON

A FARM, AN ALTERNATE WORK ANIMAL MIGHT BE A BURRO BUT THEY

ساره علاء شاكر

ARE NOT AS COMFORTABLE AS A TRANSPORT ANIMAL

بالطبع الرسالة بالأعلى هي الرسالة بعد استخدام النموذج وتعبئة كلمات الرسالة السرية، ولكي نستخرج الرسالة السرية نقوم بتطبيق قوانين النموذج لكي نحصل على:

HORSE

FERRY

SANK

IN BURLINGTON

FIND

ALTERNATE

TRANSPORT

فتكون الرسالة السرية :

-!><--[endif]! > false MicrosoftInternetExplorer4 Normal 0 false false <[if gte mso 9]--!> <--[endif]! > <[if gte mso 9]-

إخفاء المعلومات هو فنُ و علمُ و كتابة الرسائل الخفية بطريقةٍ لا تسمح لأحدٍ بالوصول إلى فهم الموجود في الرسالة، ما عدى المرسل و المتلقي المقصود، و هو شكلٌ من أشكال الأمن من خلال الغموض. تأتي كلمة *ستيجانوجرافي* من أصلٍ يوناني و تعني *"الكتابة المخفية"*. أول استخدامٍ تم تسجيله لهذا المصطلح هو في عام ١٤٩٩، و ذلك من قبل يوهانس تريثيمياس في تقريره *الستيجانوجرافيا* ، و هي أطروحة عن التشفير و إخفاء المعلومات تم تنكيرها لتبدو ككتاب عن السحر. عامة ما تبدو الرسائل كشيءٍ آخر: كصور أو مقالات أو قوائم تسوق، أو بعض الأنواع الأخرى من *النصوص الخافية* ، و تكون الرسالة المخبأة بشكل تقليدي مكتوبة بحبرٍ غير مرئي بين الخطوط الواضحة في رسالةٍ خاصة.

ميزة الستيجانوجرافي على الكريبتوجرافي (التشفير) وحده، هو أن الرسائل لا تلفت النظر إلى نفسها. فالرسائل المشفرة المرئية بوضوح -مهما كانت صعوبة فك شيفرتها- يمكن أن تثير الشكوك، و ربما تكون في حد ذاتها إدانة في البلدان التي يكون التشفير فيها أمرا غير قانوني. [١] لذا، في حين يحمي التشفير محتويات الرسالة، يقوم "إخفاء الكتابة" بحماية كل الأطراف ورسائل الاتصال.

يتضمن الستيجانوجرافي إخفاء المعلومات داخل ملفات الكمبيوتر. في الكتابة المخفية الرقمية، يمكن أن تشمل الاتصالات الالكترونية الترميز الستيجانوجرافي داخل طبقة نقل، مثل ملف وثيقةٍ أو ملف صورةٍ أو برنامجا أو بروتوكولا. و ملفات الوسائط هي مثالية للانتقال الستيجانوجرافي بسبب حجمها الكبير. كمثال بسيط، يمكن لمرسلٍ أن يبدأ بملف صورةٍ حميدةٍ ثم يقومُ بضبط اللون في كل بكسلٍ بعد مائة بكسل ليتوافق مع حرفٍ في الأبجدية، و هذا تغير ماكرٌ بحيث ألا يلحظه شخصٌ لا يبحث عنه خصيصا. لم يبحث على وجه التحديد لأنه من غير المرجح أن تلاحظ ذلك.

ساره علاء شاكر

الستيجانوجرافي القديمة

أول استخدام مسجلٍ للستيجانوجرافي يمكن إرجاعه الى ٤٤٠ قبل الميلاد عندما يذكر هيرودوت مثالين على "إخفاء المعلومات" في *تواريخ هيرودوت*. [٢] أرسل ديماراتاس تحذيرا حول هجومٍ وشيك الى اليونان عن طريق كتابته مباشرةً على الدعامة الخشبية لقرصٍ من الشمع قبل وضع سطحية شمع العسل فوقها. كانت أقراص الشمع شائعة الاستعمال في الكتابة لإمكانية إعادة استخدام سطوحها، و كان يتم أحيانا استخدامها للكتابة الاختزال. و مثالٌ قديمٌ آخرُ هو هيستييس، الذي حلق رأس عبده الذي يثق فيه أكثر من غيره، و وشم رسالةً على رأسه. و بعد نمو شعر رأسه أصبحت الرسالة مخبأة. و كان الغرض من ذلك التحريض على التمرد ضد الفرس.

التقنيات الستيجانوجرافية

الستيجانوجرافيا المادية

كان إخفاء المعلومات يستخدم على نطاق واسع، بما في ذلك العصور التاريخية الماضية و حتى يومنا هذا. التباديل الممكنة لا حصر لها و تشمل أمثلتها المعروفةُ الآتي:



Steganart سبيل المثال. ضمن هذه الصورة ، موقف خطابات رسالة خفية يتم تمثيل الأعداد المتزايدة (من ١ إلى ٢٠) ، وقيمة الرسالة التي قدمها موقفها تقاطع في الشبكة. على سبيل المثال ، أول حرف من الرسالة الخفية هو عند تقاطع ١ و ٤. لذلك ، وبعد محاولات عدة ، أول حرف من الرسالة ويبدو أن هذه الرسالة th١٤ من الأبجدية ، وآخر واحد (رقم ٢٠) هو حرف من الحروف الأبجدية th٥.

- الرسائل المخفية داخل أقراص الشمع: في اليونان القديمة، كان الناس يكتبون الرسائل على الخشب، ثم يغطونها بشمع عليه رسالةٌ أخرى بريئة.
- الرسائل الخفية على أجساد الرُسُل: كانت تستخدم أيضا في اليونان القديمة. يروي هيرودوت قصة وشمٍ مطبوعٍ على رأس عبدٍ من العبيد بعد حلق رأسه، و أصبحت الرسالة مخفيةً بعد نمو الشعر مرةً أخرى. يزعم أن الرسالة كانت تحذيرا إلى اليونان حول خطط غزوٍ فارسية. كان لهذا الأسلوب عيوبٌ واضحةٌ مثل الانتقال المتأخر في انتظار عودة الشعر بعد نموه، و إمكانية استخدام الرأس لمرةٍ واحدةٍ فقط. في الحرب العالمية الثانية، أرسلت المقاومة الفرنسية بعض الرسائل المكتوبة على ظهر السعاة بالحبر السري.
- رسائل خفية على ورقةٍ مكتوبةٍ بالأحبار السرية، في إطار رسائل أخرى أو على أجزاءٍ فارغةٍ من رسائل أخرى.
- الرسائل المكتوبة برموز مورس على الغزل ثم خياطتها على قطعةٍ من الملابس التي يرتديها ساعي.
- الرسائل المكتوبة على الجزء الخلفي من الطوابع البريدية.
- أثناء و بعد الحرب العالمية الثانية، استخدم عملاء الجاسوسيةالنقاط الدقيقة المنتجة فوتوغرافيا لإرسال المعلومات جيئةٍ و ذهابا. عادةً ما كانت النقاط الدقيقة (مايكرودوتس) أقل من حجم الحروف التي تنتجها الآلة الكاتبة. كان ينبغي وضع "المايكرودوتس" في الحرب العالمية الثانية في ورقةٍ و تغطيتها بلاصق (مثل الكولوديون). و كان هذا عاكسا للضوء،

مما يمكن قراءة الرسالة عن طريق وضعها أمام الضوء. كان من التقنيات البديلة إدراج "المايكرودوتس" في شقوقٍ تم تقطيعها في حافة البطاقات البريدية.

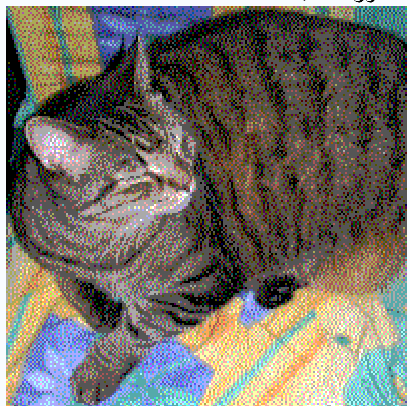
- خلال الحرب العالمية الثانية، بعث جاسوسٌ لصالح اليابان في مدينة نيويورك، فيلفالي ديكينسون، معلوماتٍ إلى عناوين مواقع محايدة في أمريكا الجنوبية. كانت العناوين لبائعة دمى، و كانت رسائلها تناقش عدد الدمى التي يجب عليها شحنها. كان النص المخفي أسماء الدمى، في حين أن النص 'المشفر' المخفي كان معلوماتٍ حول تحركات السفن، وما إلى ذلك. أصبحت قضيتها مشهورةً نوعا ما، و أصبحت تعرف باسم امرأة الدمى.
- الدعاية المضادة في الحرب البارد. في عام ١٩٦٨، كان أفراد طاقم سفينة الاستخبارات بويبلو (آجر - ٢) المحتجزين كأسرى من جانب كوريا الشمالية يبلغون رسائل بلغة الإشارة حين فرص التقاط الصور، التي تخبر الولايات المتحدة أنهم لم يكونوا منشقين بل كانوا محتجزين من قبل الكوريين الشماليين . في صورٍ أخرى تم تقديمها إلى الولايات المتحدة، أشار أفراد الطاقم "بأصابعهم" نحو الكوريين أثناء انشغالهم، في محاولةٍ لتشويه الصور التي أظهرتهم مبتسمين و مرتاحين. [٣]

الستيجانوجرافيا الرقمية


هذه مقالة عن موضوع اختصاصي يرجى من أصحاب الاختصاص أو المطلعين على موضوع المقالة مراجعة وتدقيق المقالة. *(مايو 2008)*

دخلت الستيجانوجرافيا الحديثة إلى العالم في عام ١٩٨٥ مع ظهور الكمبيوتر الشخصي و استخدامه في حل مشاكل إخفاء المعلومات الكلاسيكية. [٤] كان التطور بعد ذلك بطيئا، و لكنه انطلق كثيرا منذ ذلك الحين، بعدد برامج "الستيجو" المتاحة: تم تحديد أكثر من ٧٢٥ تطبيقا ستيجانوجرافيا رقميا من قبل مركز تحليل و أبحاث الستيجانوجرافيا. [٥] تشمل التقنيات الرقمية لإخفاء المعلومات ما يلي:


صورة شجرة. إزالة كافة ولكن بت ٢ الأخير من كل مكون من مكونات اللون تنتج صورة سوداء بالكامل تقريبا. مما يجعل تلك الصورة أكثر إشراقا وتنتج ٨٥ مرات في الصورة أدناه.


صورة قطة المستخرج من الصورة أعلاه.

- إخفاء الرسائل داخل البتات الأدنى في الصور الصاخبة أو ملفات الصوت.
- إخفاء البيانات ضمن البيانات المشفرة أو ضمن البيانات العشوائية. يتم تشفير البيانات التي يراد إخفاؤها قبل استخدامها لاستبدال جزءٍ من كتلةٍ أكبر بكثيرٍ من البيانات المشفرة أو كتلةٍ من البيانات العشوائية (فالشفرات غير قابلة للفك مثل وسادة المرة الواحدة تستطيع توليد نصوص مشفرة تبدو عشوائية تماما إذا لم يكن لديك مفتاحها الخاص).
- الممازحة و التذرية.
- تحول الوظائف المُقلِدَة ملفا واحدا لتحطيه البيانات الإحصائية لملفٍ آخرري. يمكن أن يساعد هذا الأساليب الإحصائية التي تساعد هجمات "القوة الغاشمة" في تحديد الحل الصحيح في هجوم النصوص المشفرة فقط.
- الرسائل السرية في الملفات التنفيذية التي عُبث بها، مستغلة التكرار في مجموعة تعليمات i386.
- الصور المضمنة في محتوى فيديو (و التي يمكن تشغيلها اختياريا بسرعةٍ أبطأ أو أسرع).
- حقن تأخيراتٍ غير مدركة في حزمٍ مرسلةٍ عبر الشبكة من لوحة المفاتيح. فالتأخير في الضغط على المفاتيح في بعض التطبيقات (التلنت أو البرمجيات المكتبية البعيدية) يمكن أن يعني تأخيرا في الحزم، و التأخير في الحزم يمكن استخدامه في ترميز البيانات.
- تخفي "الستيجانوجرافيا المدركة للمحتوى" المعلومات في الدلالات التي يسندها المستخدم البشري إلى حزم البيانات. توفر هذه النظم الأمن ضد الدخيل غير بشري.
- ستيجانوجرافيا البلوج. يتم تقطيع الرسائل و يتم إضافة القطع (المشفرة) كتعليقاتٍ لسجلات الشبكة المبتورة (أو اللوحات المعلقة على منصات الشبكات الاجتماعية). في هذه الحالة يعتبر اختيار البلوجات هو المفتاح المتماثل الذي يمكن للمرسل و المستلم استخدامه؛ و ناقل الرسالة الخفية هي المدونات بأكملها.

الستيجانوجرافيا المطبوعة

يمكن لمنتج الستيجانوجرافيا الرقمية أن يكون على شكل وثائق مطبوعة. يمكن أن تكون البداية *بتشفير* الرسالة، أي النص الواضح، بواسطة الوسائل التقليدية، ثم إنتاج *النص المشفر*. ثم يتم تعديل النص *الغطائي* الحميد بأي طريقةٍ لكي لا يحتوي على النص المشفر، مما يؤدي إلى تكوين *النص الستيجانوجرافي*. على سبيل المثال، يمكن التلاعب بحجم الرسالة و التباعد الذي فيها، أو بالمحرف، أو غيرها من خصائص النص الغطائي ليحملرسالة خفية. يمكن فقط للمتلقي الذي يعرف التقنية المستخدمة لاسترداد الرسالة يمكنه فك تشفيرها. طور فرانسيس بيكون شيفرة بيكون بهذا الاسلوب.

مصطلحات إضافية

بصفة عامة، يتم استخدام المصطلحات المشابهة (و المتسقة مع) تقنية الإذاعة و تكنولوجيا الاتصالات الأكثر تقليدية؛ و لكن مع ذلك، من المناسب تقديم وصفٍ موجزٍ لبعض المصطلحات التي تظهر في البرامج على وجه التحديد، والتي يسهل الخلط فيه. و هذه المصطلحات الأكثر ملاءمة لنظم الستيجانوجرافيا الرقمية.

الحمولة هي البيانات التي يراد إبلاغها سرا. *الناقل* هو الإشارة، أو التيار، أو ملف البيانات الذي تخفى فيه الحمولة؛ و هذا يختلف عن "*القناة* " (و لتي عادة ما يتم استخدمها للإشارة إلى نوع المدخلات، مثل "صورة JPEG"). يتم تسمية الإشارة أو التيار أو ملف البيانات الناتج عن ذلك الذي يحتوي على الحمولة المشفرة: "*الحزمة* " أو *ملف الستيجو* أو *الرسالة سرية*. النسبة المئوية للبايت، أو العينات أو عناصر الإشارة الأخرى التي تم تعديلها لترميز الحمولة يشار إليها بكلمة *كثافة الترميز* و يتم التعبير عنها في العادة بعددٍ بين ٠ و ١.

في مجموعة من الملفات، تسمى الملفات التي من المحتمل أن تحتوي على حمولة الملفات *المشتبه بها*. إذا تم تحديد هوية *المشتبه* عن طريق نوع من التحليل الإحصائي، يمكن أن تسمى هذه "الملفات *المرشحة* ".

التدابير المضادةيتطلب الكشف عن إخفاء المعلومات المادية الفحص البدني الحذر، بما في ذلك استخدام التكبير، و مواد التحميض و الأشعة فوق البنفسجية. و هي عملية تستغرق وقتا طويلا مع آثارٍ واضحةٍ مترتبة على الموارد، حتى في البلدان التي فيها أعدادٌ كبيرةٌ من الناس يعملون على التجسس على مواطنيهم الآخرين. و لكنه ممكنٌ مع ذلك متابعة البريد الآتي من

أفرادٍ أو بعض المؤسسات المشتبه في تورطهم، مثل السجون أو مخيمات أسرى الحرب. خلال الحرب العالمية الثانية، كان من التقنيات المستخدمة لتسهيل رصد بريد الأسرى ورقٌ معالجٌ خصيصا للكشف عن الحبر غير المرئي. في مقالٍ نشر في عدد ٢٤ يونيو ١٩٤٨ من جورنال تجارة الورق ، وصف المدير الفني لمكتب طباعة حكومة الولايات المتحدة موريس كانترويتز بعباراتٍ عامة تطور هذه الورقة، عبر ثلاثة نماذج تمت تسميتها سينسيكوت و أنيليث و كوتاليث . و كانت هذه لتصنيع البطاقات البريدية و القرطاسية التي تعطى لأسرى الحرب الألمان في الولايات المتحدة وكندا. إذا حاول أسرى الحرب كتابة رسالةٍ خفيةٍ فإن الورق الخاص من شأنه أن يجعل الكتابة مرئيا. تم منح براءتي اختراعٍعلى الأقل من الولايات المتحدة لهذه التكنولوجيا، واحدة للسيد كانترويتز، و رقمها ٢٥١٥٢٣٢ "الورق الكاشف للمياه و الورق الكاشف للتكوينات الطلائية لذلك"، و الذي حصل على براءة اختراع في ١٨ يوليو ١٩٥٠، و براءة اختراع أسبق، "الورق الحساس للرطوبة و تصنيعه"، و رقمها ٢٤٤٥٥٨٦، و حصل على براءة اختراع في ٢٠ يوليو ١٩٤٨. و هناك استراتيجية مماثلة و هي إعطاء ورق كتابةٍ للأسرى تم تسطيره بخطوط حبرٍ سائلٍ يذوب إذا لمس حبرا مائيا غير مرئي.

في مجال الحوسبة، يسمى الكشف عن حزم الستيجانوجرافية يسمى تحليل الستيجا. و لكن أبسط الطرق للكشف عن الملفات المعدلة هو مقارنتها بأصولها معروفة. على سبيل المثال، للكشف عن المعلومات التي يجري نقلها من خلال الرسومات الموجودة على موقع على شبكة الإنترنت، يمكن للمحلل الحفاظ على نسخ نظيفةٍ من هذه المواد و مقارنتها بالمضمون الراهن على الموقع. و الاختلافات إذا افترضنا أن الناقل هو نفسه، تؤلف الحمولة. بصفةٍ عامة، نجد أن استخدام معدل ضغط عالٍ للغاية يجعل من الصعب إخفاء المعلومات، و لكنه ليس أمرا مستحيلا. في حين أن الأخطاء الضغط توفر مكانا لإخفاء البيانات، فإن الضغط الشديد يقلل من كمية البيانات المتاح إخفاء الحمولة فيها، مما يزيد من كثافة الترميز و يسهل الكشف (حتى عن طريق الملاحظة العارضة في الحالات القصو).

التطبيقات

استخدامها الطابعات الحديثة

مقال تفصيلي: steganography Printer

يتم استخدام الستيجانوجرافي من بعض الطابعات الحديثة، بما فيها ماركة إتش بي و زيروكس من طابعات الليزر اللونية. يتم إضافة نقاطٍ صفراء صغيرة إلى كل صفحة. و النقاط مرئية بالكاد و تحتوي على ترميز الأرقام التسلسلية للطابعة، و كذلك طوابع التاريخ و الوقت. [٦]

مثال من الممارسة الحديثة

كلما كبر حجم الرسالة الغطائية (في مصطلح محتوى البيانات، عدد البتات) بالنسبة إلى الرسالة الخفية، يصبح من الأسهل أن تخفي الرسالة. و لهذا السبب فإن الصور الرقمية (التي تحتوي على كمياتٍ كبيرةٍ من البيانات) يتم استخدامها لإخفاء الرسائل على شبكة الإنترنت وعلى وسائط الاتصال الأخرى. من غير الواضح كمُ شيوعِ هذا الفعل. على سبيل المثال: تحتوي ملف الخارطة النقطية (أي نوع الملف بيتماب) على ٢٤ بت، و تمثل كل ٨ بتات واحدة من ثلاثة قيمٍ لونية (الأحمر والأخضر والأزرق) في كل بكسل. إذا نظرنا إلى اللون الأزرق فقط مثلا، نجد أنه سيكون هناك ٢ ^ ٨ قيم مختلفة من اللون الأزرق. و من غير المحتمل أن يتم ملاحظة الفرق بين ١١١١١١١١ و ١١١١١١١٠ في قيمة كثافة اللون الأزرق من قبل العين البشرية. ولذلك، فإنه من الممكن استخدام أقل البتات أهمية من أجل شيء آخر بخلاف المعلومات اللونية. إذا كان لنا أن نفعل ذلك مع الأخضر و الأحمر كذلك، يمكننا الحصول على حرفٍ واحدٍ من حروف الأسكي لكل ثلاثة بكسل

إذا وصفنا ذلك بشكلٍ أكثر رسمية، نقول أن الهدف لصنع ترميز الستيجانوجرافي صعب الاكتشاف هو التأكد من أن التغييرات التي أدخلت على الناقل (الإشارة الأصلية) نظرا لحقن الحمولة (الإشارة الت يراد تضمينها سرا) هي غير مذكورةٍ بصريا (و بشكلٍ مثالي من الناحية الإحصائية)؛ أي أن التغيرات لا يمكن تمييزها عن خلفية الضجيج في الناقل. يمكن لأي وسيلةٍ أن تكون ناقلا، و لكن الوسائط التي تمتلك كمياتٍ كبيرةٍ من المعلومات الزائدة عن الحاجة أو المضغوطة تلاءم هذه الوظيفة بشكلٍ أفضل.

يعني هذا من الناحية المعلوماتية النظريةأن القناة يجب أن يكون لها سعةٌ أكبر من احتياج إشارة السطحية، و يعني هذا أنه لا بد من

ساره علاء شاكر

التكرار. ففي الصورة الرقمية، قد يكون هذا ضجيجا من عنصر التصوير؛ أما الصوتيات الرقمية، فقد تكون الضوضاء من تقنيات التسجيل أو معدات التضخيم. بصفةٍ عامة، فإن الالكترونيات التي ترقمن الإشارات التناظرية تعاني من عدة مصادر ضوضاء مثل الضوضاء الحرارية و الضوضاء الوميضية و ضوضاء الضربات. يوفر هذا الضجيج ما يكفي من تفاوتٍ في المعلومات الرقمية التي تم التقاطها التي يمكن استغلالها باعتبارها ضجيجا لتغطية البيانات المخفية. بالإضافة إلى ذلك، فإن مخططات الضغط الضائعة (مثل صور JPEG) دائما تدخل بعض الخطأ في ضغط البيانات، فمن الممكن أن يستغل هذا الأمر للاستخدام الستيجانوجرافي كذلك.

يمكن أن تستخدم الستيجانوجرافيا في العلامات المائية الرقمية، حيث يتم إخفاء رسالةٍ (التي تكون مجرد مُعَرفِ) في صورةٍ بحيث يمكن تعقب المصدر أو التحقق منها